VPN Technology

Portions of this PPT draw from PPT authored by Professor Dijiang Huang at Arizona State University

Common VPN Protocols

- PPTP (Point-to-Point Tunneling Protocol)
- L2F (Layer-2 Forwarding Protocol)
- L2TP (Layer 2 Tunneling Protocols)
- PPP (Point-to-Point Protocol)
- VLAN (Virtual Local Area Networks)
- VXLAN (Virtual eXtensible LAN)
- MPLS (MultiProtocol Label Switching)
- GRE (Generic Routing Encapsulation)
- SSL (Secure Socket Layer)
- Ipsec (IP security)

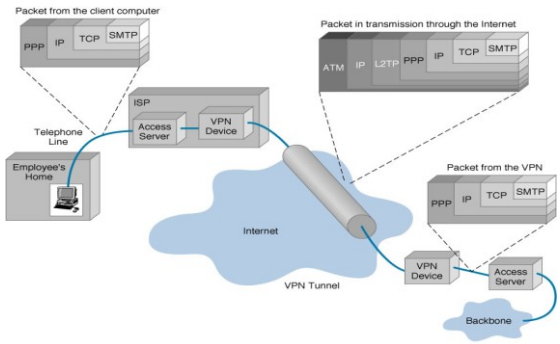
Terminology: VPN & Tunneling

- Virtual Private Network is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated connection such as leased line, a VPN uses "virtual" connections routed through the internet.
- Tunneling is the transmission of data intended for use only within a private, usually corporate network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network.
- In other words, these two terms can be interchangeable depending on where to use them.

VPN Benefits

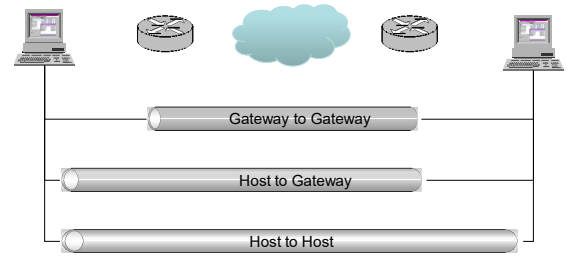
- Enable communications between corporate
  - private LANs over
    - Public networks
    - Leased lines
    - Wireless links
  - It is overlay network
- Corporate resources (e-mail, servers, printers) can be accessed securely by users having granted access rights from outside (home, while travelling, etc.)
- Software Defined Networking (SDN) has been widely using tunneling and VPN approaches.

VPN Encapsulation of Packets Example

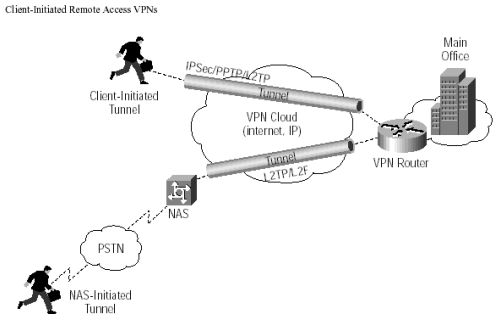


VPN Topology: Types of VPNs

- Types of VPNs
  - Remote access VPN
  - Intranet VPN
  - Extranet VPN
- Three Types of Tunnels

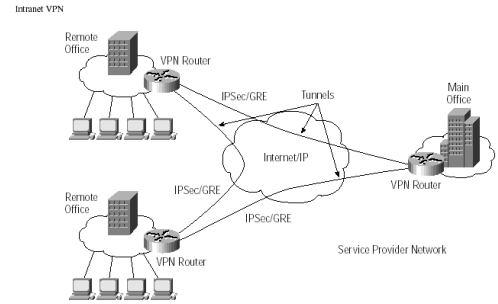


VPN Topology: Remote Access VPN

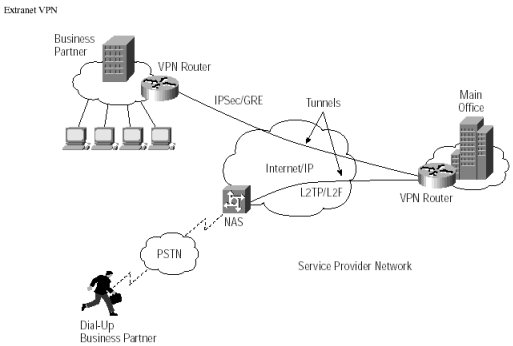


PSTN: Public Switch Telephone Networks

VPN Topology: Intranet VPN



VPN Topology: Extranet VPN



L2TP

- L2TP = L2F + PPTP
  - Combines the best features of L2F and PPTP
- Allows PPP frames to be sent over non-IP (Frame relay, ATM) networks also (PPTP works on IP only)
- Allows multiple (different QoS) tunnels between the same end-points. Better header compression. Supports flow control

Layer 2 Tunneling Protocol

- An example of network layer VPN: use IP packets to encapsulate Layer 2 frames
- Previous RFC (v2)
  - RFC2661 **Layer Two Tunneling Protocol L2TP** W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter. August **1999** (PROPOSED STANDARD)
  - A standard method for tunneling Point-to-Point Protocol (**PPP**) [RFC1661] sessions
  - **Note:** L2TP has since been adopted for tunneling a number of other L2 protocols (e.g., Ethernet, Frame Relay, etc). → L2TPv3 [RFC3931]

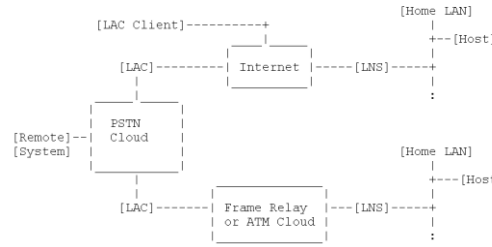
11

Layer 2 Tunneling Protocol (cont.)

- A typical L2TP scenario (from RFC2661)

2.0 Topology

The following diagram depicts a typical L2TP scenario. The goal is to tunnel PPP frames between the Remote System or LAC Client and an LNS located at a Home LAN.

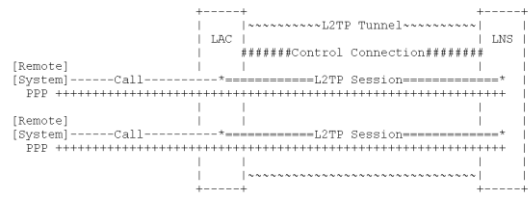


LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server)

L2TP Tunnel Setup (from RFC2661)

5.0 Protocol Operation

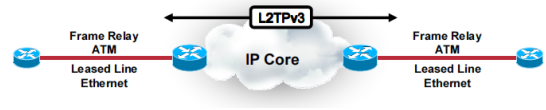
The necessary setup for tunneling a PPP session with L2TP consists of two steps, (1) establishing the Control Connection for a Tunnel, and (2) establishing a Session as triggered by an incoming or outgoing call request. The Tunnel and corresponding Control Connection MUST be established before an incoming or outgoing call is initiated. An L2TP Session MUST be established before L2TP can begin to tunnel PPP frames. Multiple Sessions may exist across a single Tunnel and multiple Tunnels may exist between the same LAC and LNS.

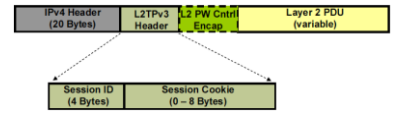


13

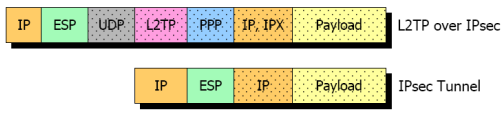
Figure 5.1 Tunneling PPP

L2TPv3 Tunneling example





L2TP-over-IPsec

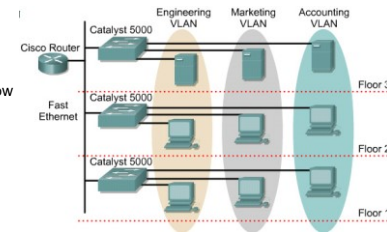


L2TP over IPsec Transport Mode vs. IPsec Tunnel Mode

15

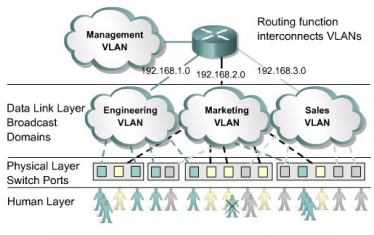
VLAN introduction

- VLANs function by logically segmenting the network into different broadcast domains so that packets are only switched between ports that are designated for the same VLAN.
  - Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.



Benefits of VLANs

- The key benefit of VLANs is that they permit the network administrator to organize the LAN logically instead of physically.



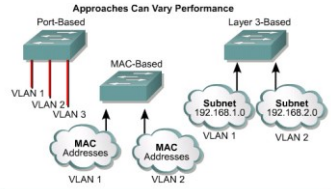
All users attached to the same switch port must be in the same VLAN.

VLAN types

- There are three basic VLAN memberships for determining and controlling how a packet gets assigned:
  - Port-based VLANs
  - MAC address based
  - Protocol based VLANs
- The frame headers are encapsulated or modified to reflect a VLAN ID before the frame is sent over the link between switches.
- Before forwarding to the destination device, the frame header is changed back to the original format.

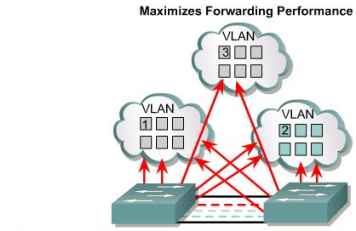
VLAN types

- Port-based VLANs
- MAC address based VLANs
- Protocol based VLANs



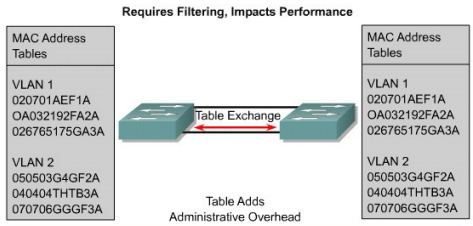
VLAN Types	Description
Port-based	• Most common configuration method. • Ports assigned individually, in groups, in rows, or across 2 or more switches. • Simple to use. • Often implemented where Dynamic Host Control Protocol (DHCP) is used to assign IP addresses to network hosts.
MAC address	• Rarely implemented today. • Each address must be entered into the switch and configured individually. • Users find it useful. • Difficult to administer, troubleshoot and manage.
Protocol Based	• Configured like MAC addresses, but instead uses a logical or IP address. • No longer common because of DHCP.

Membership by Port



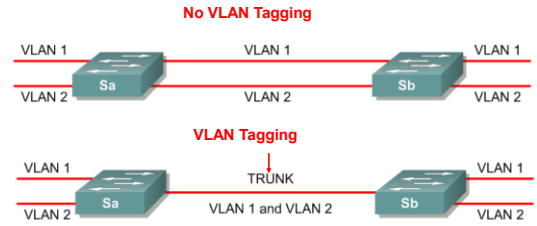
- User assigned by port association
- Requires no lookup if done in ASICs
- Easily administered via GUIs
- Maximizes security between VLANs
- Packets do not "leak" into other domains
- Easily controlled across network

Membership by MAC-Addresses



- User assigned based on MAC addresses
- Offers flexibility, yet adds overhead
- Impacts performance, scalability, and administration
- Offers similar process for higher layers

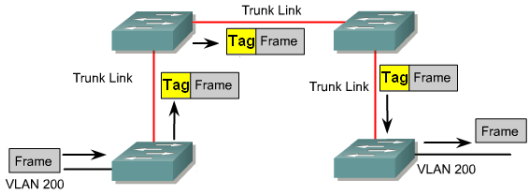
VLAN Tagging



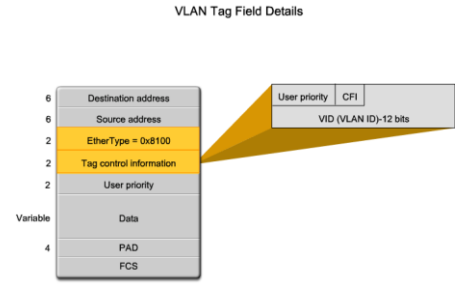
- VLAN Tagging is used when a single link needs to carry traffic for more than one VLAN.

Tag to identify VLAN

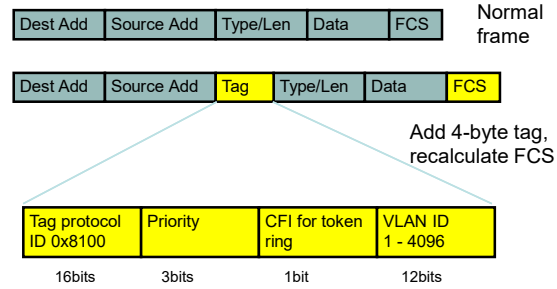
- Tag is added to the frame when it goes on to the trunk
- Tag is removed when it leaves the trunk



VLAN Trunk - 802.1Q Frame tagging



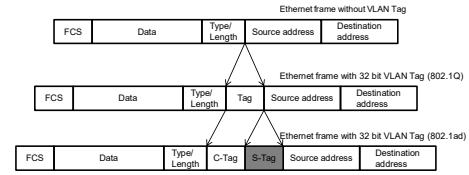
Frame tagging IEEE 802.1Q



Frame Check Sequence (FCS)

VLAN 802.1ad (QinQ)

- Provider Bridge (IEEE 802.1ad)
  - Two VLAN tags and hence called Q-in-Q



VXLAN: VLANs for data centers

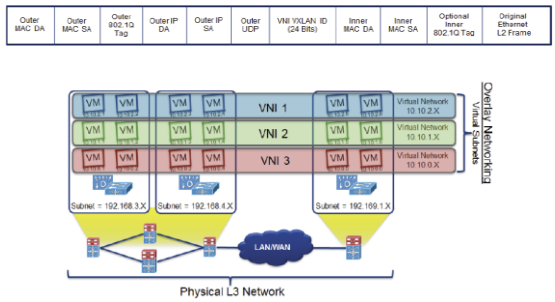
- Prior IEEE 802.1Q standard: 12 bits = 4094 VLANs
- What if each tenant in datacenter wants isolated subnet?
  - Quickly run out of VLAN ids
  - VLANs need to all be in same Ethernet SP, doesn't scale
- Enter VXLAN:
  - 24 bit VLAN ids
  - Bridge multiple layer-3 subnets, using MAC-in-IP tunneling
  - Give impressive of single large layer-2 subnet per tenant
- Enable establishing VLAN through Internet
- Backed by VMWare + Cisco
  - http://tools.ietf.org/html/draft-mahalingam-dutt-dcops-vxlan-00

27

What is VXLAN?

- At its core, VXLAN is simply a MAC-in-UDP encapsulation (in other words, encapsulation of an Ethernet L2 Frame in IP) scheme enabling the creation of virtualized L2 subnets that can span physical L3 IP networks.
- VXLAN enables the connection between two or more L3 networks and makes it appear like they share the same L2 subnet.
- It allows virtual machines to operate in separate networks while operating as if they were attached to the same L2 subnet.

VXLAN Ethernet Frame Encapsulation



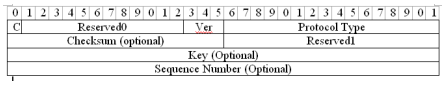
Generic Routing Encapsulation (GRE)

- Provides low overhead **tunneling** (often between two private networks)
- Does not provide encryption
- Used to encapsulate an arbitrary layer protocol over another arbitrary layer protocol:
  delivery header + GRE header + payload packet
- Mostly IPv4 is the delivery mechanism for GRE with any arbitrary protocol nested inside
  e.g., IP protocol type 47: GRE packets using IPv4 headers
- RFCs:
  - RFC1701 **Generic Routing Encapsulation (GRE)** S. Hanks, T. Li, D. Farinacci, P. Traina, October 1994 (INFORMATIONAL)
  - RFC2784 **Generic Routing Encapsulation (GRE)** D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, March 2000 (PROPOSED STANDARD)
  - RFC2890 **Key and Sequence Number Extensions to GRE** G. Dommety, September 2000 (PROPOSED STANDARD)

30

Generic Routing Encapsulation

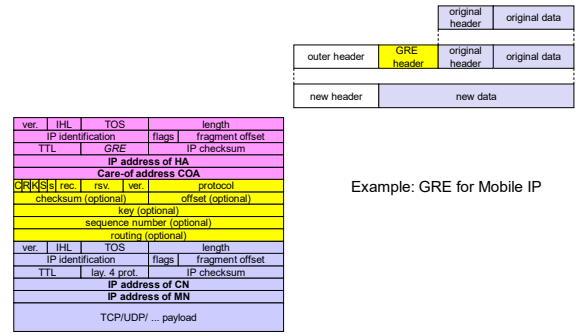
- GRE Header (based on RFC1701, deprecated): Figure 11-2
- GRE Header (based on RFC 2784 & 2890): Figure 11-4



- C = 1, checksum present
- Checksum: to ensure the integrity of the GRE header and the payload packet; contains a checksum of the GRE header and the payload packet
- Key:
  - contains a number to prevent misconfiguration of packets;
  - may be used to identify individual traffic flow within a tunnel
  - Not the same as a cryptographic key

31

Generic Routing Encapsulation Example



Example: GRE for Mobile IP

6.32

Generic Routing Encapsulation

- Summary:
  - GRE mainly perform 'tunneling'.
  - Does not provide a means to securely encrypt its payload
  - Often relies on application layer to provide encryption
  - May be used together with a network layer encryption (such as IPsec)

    Example 1: use GRE to encapsulate non-IP traffic and then encrypt the GRE packet using IPsec

    Example 2: use GRE to encapsulate multicast traffic, and then encrypt the GRE packet using IPsec

    Question: Why not simply use IPsec?

33